

FORM PTO-1390  
(REV. 11-2000)

U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

ATTORNEY'S DOCKET NUMBER

7157306-0241

TRANSMITTAL LETTER TO THE UNITED STATES  
DESIGNATED/ELECTED OFFICE (DO/EO/US)  
CONCERNING A FILING UNDER 35 U.S.C. 371

U.S. APPLICATION NO. (If known, see 37 CFR 1.5)

09/936410

INTERNATIONAL APPLICATION NO.  
PCT/DE00/00586INTERNATIONAL FILING DATE  
02 March 2000PRIORITY DATE CLAIMED  
12 March 1999

TITLE OF INVENTION

ANONYMIZATION METHOD

APPLICANT(S) FOR DO/EO/US

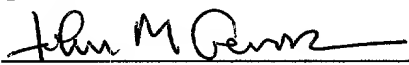
Roland Nehl

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☐ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9) and (21) indicated below.
4. ☐ The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
  - a. ☒ is attached hereto (required only if not communicated by the International Bureau), including 4 sheets of drawings (fig. 1-5)
  - b. ☐ has been communicated by the International Bureau.
  - c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☒ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
  - a. ☒ is attached hereto, including 5 sheets of drawings (fig. 1-5)
  - b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
7. ☐ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
  - a. ☐ are attached hereto (required only if not communicated by the International Bureau).
  - b. ☐ have been communicated by the International Bureau.
  - c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
  - d. ☐ have not been made and will not be made.
8. ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371 (c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)). - unsigned
10. ☐ An English language translation of the annexes of the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

## Items 11 to 20 below concern document(s) or information included:

11. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☐ A FIRST preliminary amendment.
14. ☐ A SECOND or SUBSEQUENT preliminary amendment.
15. ☐ A substitute specification.
16. ☐ A change of power of attorney and/or address letter.
17. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.
18. ☐ A second copy of the published international application under 35 U.S.C. 154(d)(4).
19. ☐ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
20. ☒ Other items or information:  
copy of the international search report mailed 11/09/2000

U.S. APPLICATION NO. (if known) <b>09/936410</b> INTERNATIONAL APPLICATION NO. <b>PCT/DE00/00586</b>		ATTORNEY'S DOCKET NUMBER <b>7157306-0241</b>	
21. <input type="checkbox"/> The following fees are submitted: <b>BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)):</b> Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO. .... <b>\$1000.00</b>  International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO ..... <b>\$860.00</b>  International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO ..... <b>\$710.00</b>  International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4) ..... <b>\$690.00</b>  International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4) ..... <b>\$100.00</b>  <b>ENTER APPROPRIATE BASIC FEE AMOUNT =</b>		<b>CALCULATIONS PTO USE ONLY</b>	
Surcharge of <b>\$130.00</b> for furnishing the oath or declaration later than <input type="checkbox"/> 20 <input type="checkbox"/> 30 months from the earliest claimed priority date (37 CFR 1.492(e)).		\$ 860	
CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE
Total claims	- 20 =		x <b>\$18.00</b>
Independent claims	- 3 =		x <b>\$80.00</b>
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ <b>\$270.00</b>
<b>TOTAL OF ABOVE CALCULATIONS =</b>		<b>\$ 1130</b>	
<input type="checkbox"/> Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by 1/2.		+	
<b>SUBTOTAL =</b>		\$	
Processing fee of <b>\$130.00</b> for furnishing the English translation later than <input type="checkbox"/> 20 <input type="checkbox"/> 30 months from the earliest claimed priority date (37 CFR 1.492(f)).		\$	
<b>TOTAL NATIONAL FEE =</b>		<b>\$ 1130</b>	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). <b>\$40.00</b> per property +		\$	
<b>TOTAL FEES ENCLOSED =</b>		\$	
		Amount to be refunded:	\$
		charged:	\$ <b>1130</b>
a. <input type="checkbox"/> A check in the amount of \$ _____ to cover the above fees is enclosed. b. <input checked="" type="checkbox"/> Please charge my Deposit Account No. <u>23-1703</u> in the amount of \$ <u>1130</u> to cover the above fees. A duplicate copy of this sheet is enclosed. c. <input checked="" type="checkbox"/> The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. <u>23-1703</u> . A duplicate copy of this sheet is enclosed. d. <input type="checkbox"/> Fees are to be charged to a credit card. <b>WARNING:</b> Information on this form may become public. <b>Credit card</b> <b>information should not be included on this form.</b> Provide credit card information and authorization on PTO-2038.			
<b>NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137 (a) or (b)) must be filed and granted to restore the application to pending status.</b>			
SEND ALL CORRESPONDENCE TO: Customer No. 007470		 SIGNATURE  <u>John M. Genova</u> NAME  <u>32,224</u> REGISTRATION NUMBER	

207220-0749660

JC03 Rec'd PCT/PTO 12 SEP 2001

WO 00/56005

PCT/DE00/00586

Anonymization method

The invention relates to a method for anonymizing sensitive data within a data stream.

5

Information for long-term storage is stored in databases. The value of such information collections is considered to be an essential asset of organizations. Owing to the sensitivity, access to databases is generally restricted, i.e. access is possible only for authorized users in accordance with their user rights profiles. In a user rights profile it is possible to define who can access which data in which modes (for example reading, writing). A current example is when it is not possible for every employee of a company to access personnel data. It is also possible for employees to access, on a "need-to-know" principle, only that information which they require to carry out their duties. All other information is barred. An administrator is responsible for allocating the access rights, and the reliability of the data protection depends essentially on this administrator.

To provide data security, anonymization methods are frequently used which anonymize the data which is not to be accessed. Such methods are used in particular if data is to be transferred to a database in the form of a data stream, in which case it is necessary to ensure that there is no unauthorized access to the data on the transmission path. An application example of this is the dispatch of a data stream by e-mail. Transmitters and receivers then have full access rights to all the data contained in the database. The data is encrypted before transmission so that attackers within the Internet cannot access the data. The receiver decrypts the data, and can access it completely.

WO 00/56005

- 2 -

PCT/DE00/00586

In the known methods for protecting databases, authorization and testing of user rights is typically performed at the front end of the database. This applies, for example, to DB2<sup>TM</sup> from IBM. If a higher  
5 level of user access rights is required, there are commercial products, for example RACF<sup>TM</sup> (Resource Access Control Facility) from IBM. However, access control is also performed here by an administrator.

10 A classic situation in which the conventional methods are inadequate is an outsourcer/insourcer relationship. An outsourcer has certain services provided by an insourcer and provides the insourcer with all the data necessary to do so, said data being stored in a  
15 database at the insourcer's end. If, for data protection reasons or for reasons of customer protection, the outsourcer wishes itself to control the dissemination of customer-identifying data, the known anonymization methods are used either to prevent access  
20 to the entire database or to place the selective control of access to specific data under the aegis of an administrator which is located at the insourcer's premises. Therefore, it would basically also be possible to access sensitive data.

25 The object of the present invention is to make available a method which permits a database to be accessed, but excludes certain data within this database from access without destroying the  
30 relationship between the excluded data and the rest of the data. It should be possible to transfer the database to third parties for processing of the non-protected data, without losing control of access to the protected data.

35 According to the invention, a method for anonymizing sensitive data within a data stream is proposed, having the following steps:

09.09.01 10:03:10 201220074950

WO 00/56005

- 3 -

PCT/DE00/00586

- a) the sensitive date field is compressed,
- b) the sensitive data field is anonymized,
- 5 c) the anonymized sensitive data field is marked within the data stream by means of start and stop characters.

10 According to the invention, the sensitive data is selectively anonymized within a database. The anonymized data fields are provided with a start character and a stop character in order to identify them for later de-anonymization.

15 The method according to the invention can be used in particular when a database user stores data in a database, and some of the data items are to be processed by a database operator. While the database user is authorized to read all the data, sensitive data, for example customer-identifying information, is to be anonymized as far as the database operator is concerned, and it is to be impossible for said database operator to de-anonymize said information. The

20 anonymization information remains with the database user. The non-anonymized data can be evaluated and processed by the database operator. The relationship between the data remains unchanged.

25 The sensitive data can be, for example, customer-identifying information, and it is to be possible for the data assigned to the customer to be read for the purpose of statistical evaluation. The database can be partially anonymized with the anonymization method

30 according to the invention and passed on to third parties for statistical evaluation and processing. The customer-identifying data cannot be read by the third party. The control over which user access rights are

WO 00/56005

- 4 -

PCT/DE00/00586

assigned to which persons remains with the database user. The relationship between the processed data and the respective anonymized data, such as customer name, remains unchanged. After the evaluated or processed database is returned to the database user, the database user can perform a de-anonymization and use the entire processed database.

The method according to the invention can, in particular, be applied advantageously even if the sensitive data fields have a predefined field length. However, it is self-evident that the method can also be appropriately applied without restriction when there are unlimited field lengths. Even if the following statements relate increasingly to sensitive data fields of a predefined field length, this is not to be understood as restrictive.

The data can advantageously be compressed before the sensitive data field is anonymized. In the case in which the data field is completely filled, this provides the space for the addition of start and stop characters for marking the anonymized data field. The marking is necessary for later de-anonymization of the data field.

If, in any case, the data field is not completely filled, or if the data is compressed by the compression to such an extent that there is still space remaining in the data field, the data field can be filled in by fill characters before the anonymization.

There are, in particular, two possible methods available for anonymizing the data field, namely pseudonymization and encryption.

If the data field is completely filled, pseudonymization is preferably performed. To do this,

WO 00/56005

- 5 -

PCT/DE00/00586

the length of the pseudonym used has to be selected in such a way that space remains for start and stop characters in the data field after the pseudonymization.

5

If there is still space within the data field, the data field is preferably at least partially filled by fill characters, in particular with random values, and subsequently encrypted.

10

Filling the field with random values ensures that isonomies are resolved. For example, it is necessary that frequently occurring names, such as Müller, Meier etc. in the German-speaking world are encrypted differently so that by analyzing the frequency of the data it is not possible to draw conclusions about the data. This is done by filling the data field with random values and subsequently encrypting it.

15

20

In a preferred embodiment of the method according to the invention, information relating to the key used for the encryption is also stored in the encrypted data field. This key information has the purpose of enabling the database user to decrypt the encrypted data. In this way, it is possible to use various keys for encrypting the data, the corresponding key information for identifying the key being stored in each case within the field. Of course, the filling level of the field must be carried out in such a way, or generated by means of data compression in such a way that space remains for storing key information.

25

30

35

The detection of which data is encrypted or decrypted can be implemented by clearly marking what is referred to as start and stop characters, such as "{" and "}". In the system in question, it is not permitted to use the start and stop characters apart from for marking encrypted data. This approach has the advantage that it

WO 00/56005

- 6 -

PCT/DE00/00586

is independent of the applications which operate on the data.

If there is no single unambiguous start character in the system in question, a set start character can be used. The same applies to the stop characters. In the simplest case, the set start character could be composed of a character which is identical to the stop character. However, this has in turn the disadvantage that synchronization in a fault situation is no longer possible solely on the basis of the knowledge of start and stop characters.

The method according to the invention is explained in more detail below by means of various examples and with reference to the appended figures, in which:

Figure 1 shows the marking of sensitive data which is to be anonymized;

Figure 2 shows the flowchart of an encryption and/or decryption process;

Figure 3 shows the flow of an encryption process;

Figure 4 shows the structure of an encrypted data field;

Figure 5 shows the flow of a decryption process.

The anonymization method should fulfill the following requirements:

1. Frequently occurring data (for example the frequently occurring names Müller, Meier etc. in the German-speaking world) should be encrypted differently. This is intended to prevent conclusions being able to be drawn about the data



WO 00/56005

- 7 -

PCT/DE00/00586

itself by analyzing the frequency of data. The intention is to resolve the isonomies in the data.

2. The length of a data field to be encrypted is restricted by a fixed maximum length which is predefined essentially by the database design. Field types, for example numeric or alpha numeric, must not be changed. This requirement permits subsequent integration of the method without an operator of a database system having to change his applications in order to process the data.

3. Each encrypted data field contains all the information, apart from keys and systemwide parameters, for decryption. It is therefore possible to process each data field independently.

The aforesaid three properties are to be fulfilled simultaneously by the selected anonymization method.

In order to carry out the method, the filling level (compression ratio) of the data field to be anonymized is firstly checked. It must be ensured that there is still sufficient space within the predefined fixed data field length after the encryption in order to store a start character and a stop character and information for the key used.

If the filling level of the data field is too high to be able to carry out encryption with the aforesaid criteria, the data field is firstly compressed. If the compression of the data field does not give rise to a sufficiently small field size either, pseudonymization is carried out. The pseudonym must be selected in such a way that the condition predefined under 2.) in terms of the filling level of the data field is fulfilled.

WO 00/56005

- 8 -

PCT/DE00/00586

If the filling level of the data field is sufficiently small to permit encryption of the data field, the encryption is performed. To do this, the data field is firstly filled to the maximum possible filling level with random values.

When the information content of the data field is small, data compression can be performed before the filling in order to be able to resolve isonomies better.

The encryption is then performed. The encryption algorithm used can be selected as desired. Current algorithms are, for example, IDEA (International Data Encryption Algorithm) or DES (Data Encryption Standard).

The encrypted data field is then marked with a start character and a stop character. In addition, information relating to the key used for the encryption is stored in the data field at a previously defined position.

The following example will illustrate the method:

The data field length is 40 characters. The content of the unencrypted data field is the name "Meier". "{" is used as the start character, and "}" is used as the stop character. The data field is filled to the full field length and provided with start and stop characters, that is to say:

{Meier.....}.

The 40 characters between the start and stop characters are processed by the method. The encryption then results in a 40 character-long data field including the start and stop characters, that is to say for example:

WO 00/56005

- 9 -

PCT/DE00/00586

{ch74nHhdjqa.....yjas8}.

In the encrypted data fields, k bits are provided for marking the key used from a key set. It is thus possible to represent  $2^k$  different keys. As a result of additional information being incorporated into the encrypted data fields, for example set start characters, key bits and information relating to the initialization sector used for the encryption algorithm, it is necessary to compress the data fields which are to be encrypted.

In the appended figure 2, the encryption and decryption of data fields is illustrated. The individual steps are explained in more detail below.

The description of the method depends on the following conditions:

- Each character is represented by a byte (for example ASCII or EBCDIC code). Before the encryption or decryption, all the characters of a field are converted into an internal character set (ASCII) and then converted again appropriately.

- The different parameters are defined as follows:

1. a character set (for example 91 specific characters of the EBCDIC code);

2. a set of the start characters and stop characters for encrypted data fields, which are not included in the character set;

3. an alternative character for characters which do not belong to the character set (is part of the character set);

WO 00/56005

- 10 -

PCT/DE00/00586

4. possibly necessary fill characters (is part of the character set);

5. method parameters for the compression process;

6. information on how the original data field is to be subsequently processed as when compression is not successful;

7. information on the representation of bit sequences as sequences of permissible characters;

8. information on which of the keys from the key set is to be used.

Depending on the power of the character set, individual bit segments can each be converted to form character sequences of a specific length (for example, given a character set of 91 characters, every 13 bits can be respectively converted effectively into two characters). The best would be to perform a "common" conversion of the entire bit sequence by considering the sequence as a binary number and representing this number in the base  $b = \text{power of the character set}$ .

A method for effectively encoding on as large as possible bit sequence into a data field of a predefined length, which data field is provided for implementation on systems with 32-bit processors, is described below. Firstly, for a given character set of the size  $b$  the following is calculated once before the basic initialization (" $\ln$ " represents here the natural logarithm):

WO 00/56005

- 11 -

PCT/DE00/00586

- the minimum value of  $x/y$  is determined for integral  $y$  from 1 to 32 and integral  $x \geq y \cdot \ln(2)/\ln(b)$ .

For example: when  $b = 91$ , a minimum is obtained when  $x = 2$  and  $y = 13$ .

- for all values  $x'$  of 1 to  $x-1$ , the respective integral maximum  $y'(x')$  is calculated by means of  $y'(x') \cdot \ln(2)/\ln(b) \leq x'$ . In addition,  $y'(0) = 0$  is selected.

Example: when  $b = 91$  and  $x = 2$ , the following is obtained  $y'(1) = 6$ .

A bit sequence can then be converted into a data field of the length  $d$  as follows:

- In each case  $y$  bits are converted into in each case  $x$  characters.  
Example: when  $b = 91$ , every 13 bits are replaced by 2 characters each.
- If the given data field length  $d$  cannot be divided by  $x$ ,  $y'(x')$  bits are converted into the remaining  $x'$  characters. In the example, 6 bits are also represented by a character.

If  $s$  is assumed to be the number of start characters used in the encrypted data field and

$$L(d,b,s) = L((d-s-1) \text{DIV } x) * y + y'((d-s-1) \text{MOD } x)$$

will be assumed to be the number of bits which can be converted into a data field of the length  $(d-s-1)$  by applying the above method. The value  $(d-s-1)$  results from the fact that the set of start characters of the length  $s$  and the stop character must be included in the encrypted data field.

20220410 09:40

WO 00/56005

- 12 -

PCT/DE00/00586

When  $d = 30$ ,  $b = 91$  and  $s = 1$ , the following is obtained for example  $L = 14 * 13 + 0 = 182$ , when  $d = 15$ ,  $b = 91$  and  $s = 3$ ,  $L = 5 * 13 + y'(1) = 65 + 6 = 71$ .

5

Let  $m = (L - k - \text{length of compressed bit sequence})$ . The bits still available after the compression,  $k$  bits are provided for the number of the key used. All sorts of methods can be used for the compression. Depending on this number  $m$ , it is defined how the initialization vector will be made available for the encryption and coded.

10

15

The suitable selection of the initialization vector ensures that isonomies are resolved. In principle, the following possibilities can be used for this:

- use of random numbers

20

- use of counters

Various keys of the key set composed of  $k$  keys can be used with staggered timing. During the encryption it is necessary to define which of these keys is to be used.

25

The key number is encoded by  $k$  bits.

If the bit sequence composed of  $k$  bits for the number of the key, the bits for the encoding of the initialization vector and the bits for the compressed data field should be shorter than necessary, i.e. smaller than  $L$ , it is filled in at the end with "0" bits until the maximum admissible bit length  $L$  is reached.

30

35

The compressed data field content is encrypted.

The encryption can be carried out with a block encryption algorithm and the stored secret key in the

20220704 09:40:00

WO 00/56005

- 13 -

PCT/DE00/00586

CBC mode, the last block of the length  $j$  (if this is shorter than 64 bits) being encrypted in the CFB mode (see for example ISO/IEC 10116, Information Technology - Modes of Operation for an  $n$ -bit Block Cipher Algorithm, 1991).

In the consideration it is assumed that the typical block length of 64 is used. It is clearly possible to generalize to other block lengths. In another variant, what is referred to as stream cipher algorithms, could be used directly for character-by-character encryption.

Finally, in order to form the encrypted data field the character sequence which is obtained is inserted between the set start character and the stop character.

As soon as the start character sequence is detected in the data stream, the subsequent characters are input into an internal memory until the stop character appears.

If the start character sequence is among the subsequent characters, the process of storing is terminated and started at the new start character sequence. If a stop character has still not been detected after a predefined maximum length, the process is also terminated and the next start character sequence is looked for again. If there are fewer than a predefined lower limit of characters between the set start character and the stop character, the storage is also terminated.

Not every data field can be compressed to such an extent that the desired number of bits is available for the initialization vector. The shorter the data set length, the worse the compression, with the consequence that fewer bits are available for the initialization

WO 00/56005

- 14 -

PCT/DE00/00586

vector and there are thus fewer possible ways of generating various ciphertexts for a data field.

In such a case, there are in principle the following  
5 three possible ways of continuing:

1. Shortening the data field until sufficient compression can be achieved. However, this is inevitably associated with loss of information.
- 10 2. The affected data field is not encrypted, and it will thus remain in plain text. This can possibly be acceptable if this occurs rarely in relation to the overall set of data fields to be encrypted.
- 15 3. Use of the pseudonymization approach, which is described below.

It may be found that no adequate compression of the data records can be achieved when there is a predefined fixed field length. If shortening or passing on in plain text is not acceptable, the complete "masking" of all the selected data records can be implemented by means of the pseudonymization approach.

25 Data fields and pseudonyms can be linked, and vice versa, in a way analogous to an alias. The information is contained in a table.

30 Leutheusser-Schnarrenberger <-> X1BXE.....H

Garmisch-Partenkirchen <-> X2BXD9.....Z

If the pseudonymization is necessary at a plurality of  
35 spatially separated locations, the pseudonyms which are allocated to all the locations must be reserved at all the other locations (replication). This means



WO 00/56005

- 15 -

PCT/DE00/00586

additional communication costs. Additional measures for protecting the transmission are necessary.

The encrypted data fields can be stored over relatively long time periods, for example 5 to 15 years. The use of different keys staggered over time is advisable for the following reasons:

- If the key becomes known, the entire set of encrypted data fields must be considered as being exposed.
- The set of encrypted data fields which is available to a crypto analyst is significantly smaller if a plurality of keys are used.

For this reason, the method provides k keys for each set of database users which cooperate.

The keys can be generated in a trust center (trustworthy third-party entity) which makes available the necessary technical and organizational environment.

Various sets of database users which do not cooperate with one another should have various sets of keys which do not have any dependence on one another. This excludes the possibility of a set of database users being able to access database information from the other set of database users.

The key management is composed of the following functions:

1. Generation of keys

A key packet composed of k keys is generated. A hardware random number generator is particularly suitable for this. In the operation after the

WO 00/56005

- 16 -

PCT/DE00/00586

generation of the keys, the generated keys can be stored on a key storage medium, for example a smart card or PCMCIA card. These media can be configured in such a way that they carry out the cryptographic calculations themselves, or issue keys only after authentication has been performed.

2. Distribution of keys.

From the location where the keys are generated, the keys can be transported on a key storage medium to the place of use (terminal) or to a secure place of storage (back-up).

3. Introducing keys into terminals

A terminal is defined by the fact that it can carry out the necessary encryption and decryption processes. Such a device can be a specially developed piece of hardware or a PC. The keys can be loaded into a terminal from the key storage medium after prior authentication has been performed, or the terminal can receive orders to perform encryption and decryption. The latter case requires a corresponding resource of the key storage medium, but has the advantage that the keys never leave the key storage medium.

4. Destroying keys

If a cooperating set of database users no longer requires a key package composed of k keys, it is possible to destroy the keys by means of suitable measures, for example by destroying the key storage medium and deleting the key package from the corresponding terminals, if present.

WO 00/56005

- 17 -

PCT/DE00/00586

**Patent Claims**

1. A method for anonymizing sensitive data within a data stream, having the following steps:
  - a) the sensitive data field is compressed,
  - b) the sensitive data field is anonymized,
  - c) the anonymized sensitive data field is marked within the data stream by means of start and stop characters.
2. The method as claimed in claim 1, characterized in that the sensitive data field is filled up by fill characters before the anonymization.
3. The method as claimed in claim 1 or 2, characterized in that the data to be anonymized is pseudonymized.
4. The method as claimed in claim 1 or 2, characterized in that the data to be anonymized is encrypted.
5. The method as claimed in claim 4, characterized in that sensitive data fields are at least partially filled in with random values before the encryption.
6. The method as claimed in claim 4 or 5, characterized in that information relating to the key to be used for the encryption is stored in the encrypted data field.
7. The method as claimed in one of claims 1 to 6, characterized in that the sensitive data field has a fixed field length.

09/936410

WO 00/56005

PCT/DE00/00586

1/5

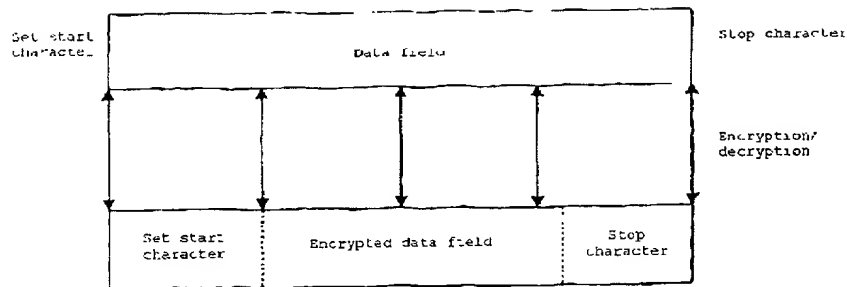


Fig. 1

09/936410-028

09/936410

WO 00/56005

PCT/DE00/00586

2/5

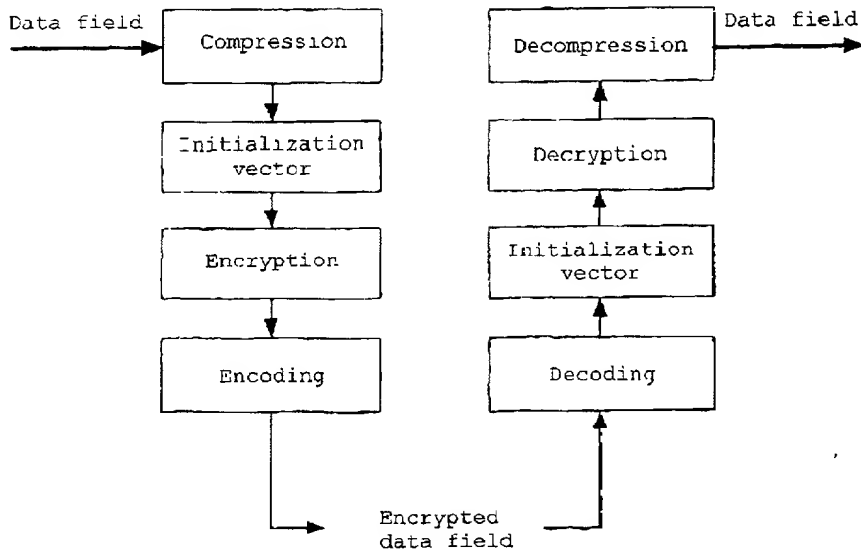


Fig. 2

2012220" 01492660

09/936410

WO 00/56005

PCT/DE00/00586

3/5

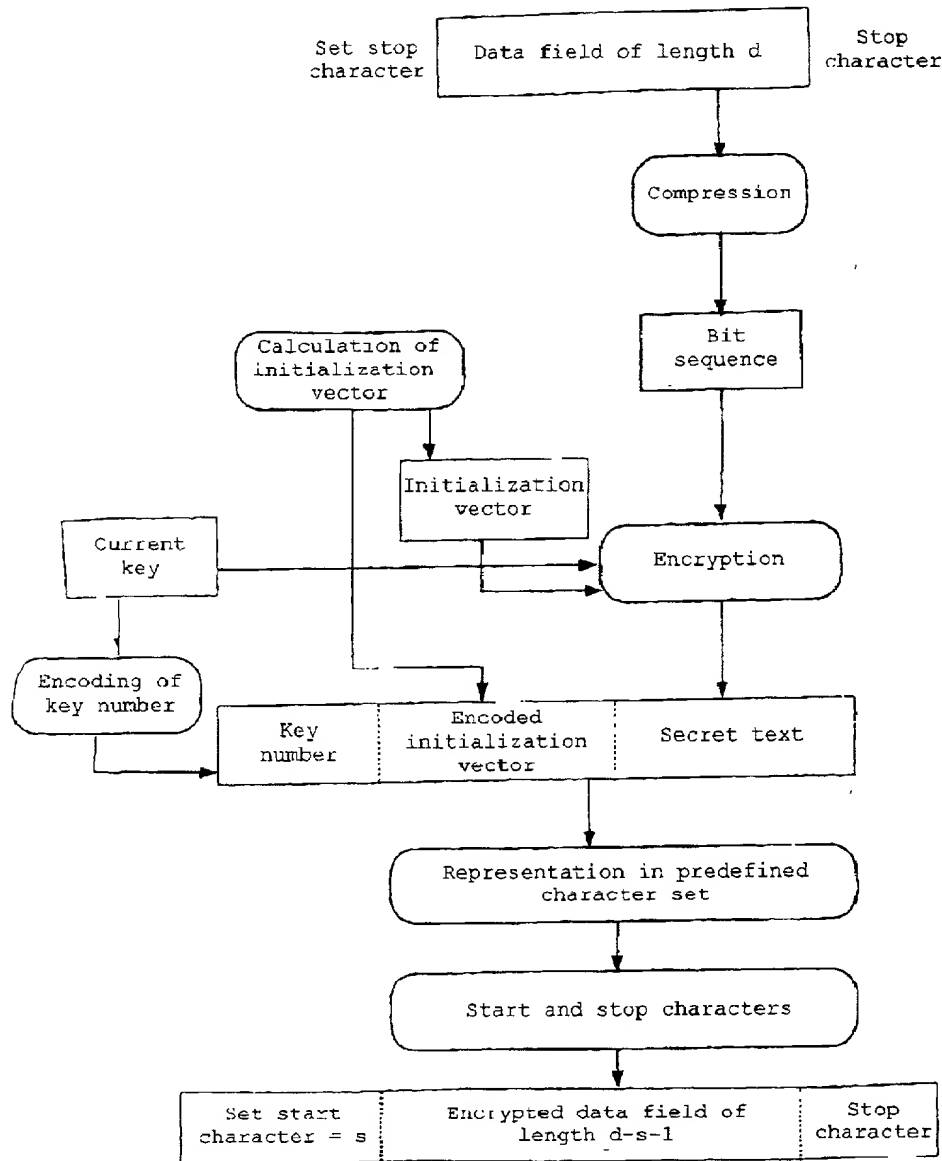
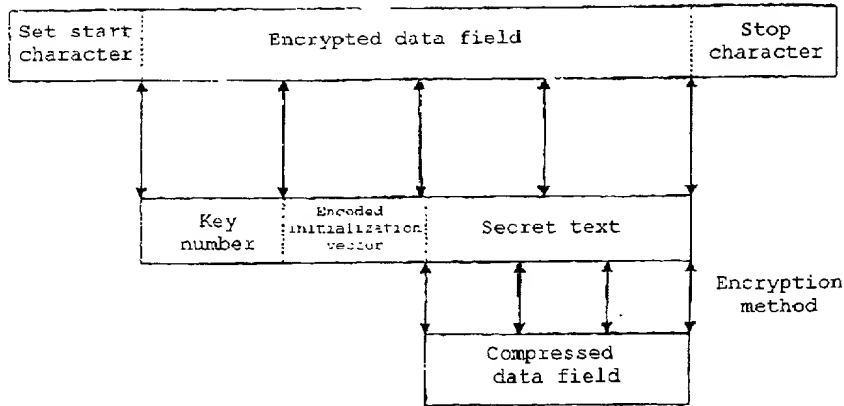


Fig. 3

WO 00/56005

PCT/DE00/00586

4/5



**Fig. 4**

09/936410

WO 00/56005

PCT/DE00/00586

5/5

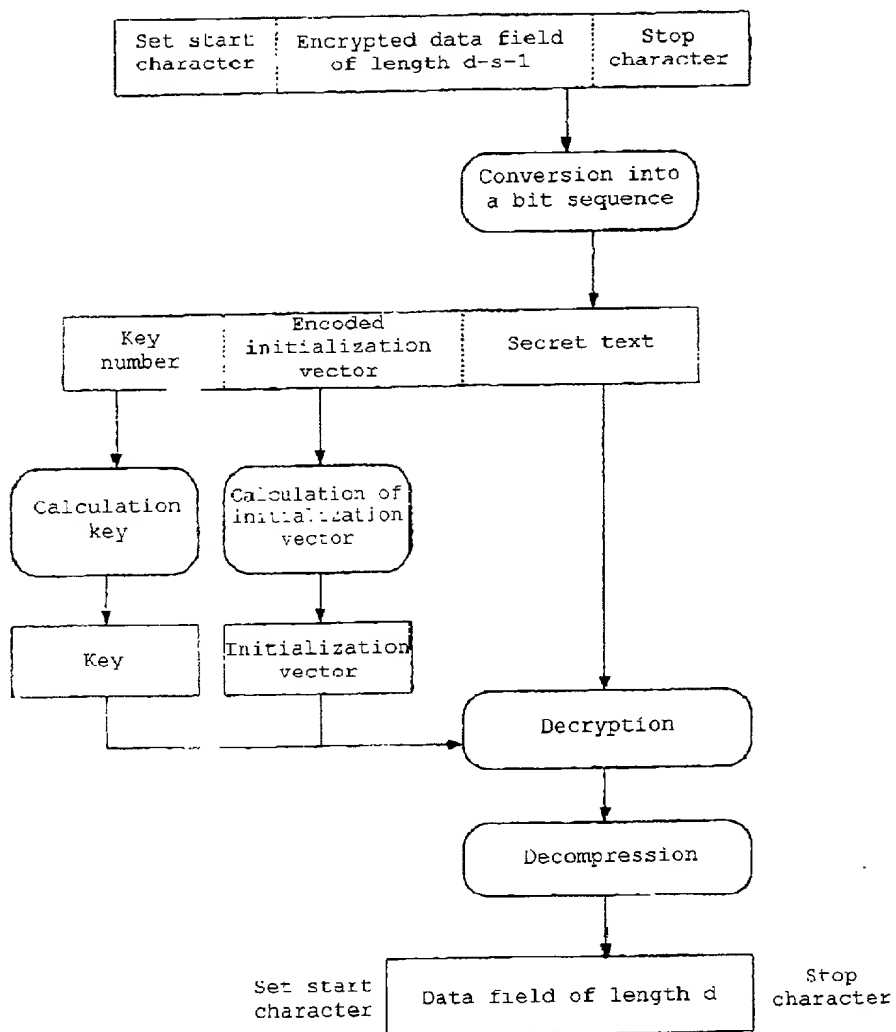


Fig. 5



JC10 Rec'd PCT/PTO 21 FEB 2002

Docket Number: 7157306-0241

**DECLARATION FOR PATENT APPLICATION**

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

the specification of which is attached hereto unless the following box is checked:

☒ was filed on 02 March 2000 as United States Application Number \_\_\_\_\_  
or International Application Number PCT/DE/00/00586 and was amended on \_\_\_\_\_  
(if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR § 1.56.

I hereby claim foreign priority benefits under 35 U.S.C. § 119(a)-(d) or § 365(b) of any foreign application(s) for patent or inventor's certificate, or § 365(a) of any PCT international application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or of any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)

Priority Not Claimed

<u>199 11 176.6</u>	<u>DE</u>	<u>12 March 1999</u>
Number	Country	Day/Month/Year Filed

Number	Country	Day/Month/Year Filed
--------	---------	----------------------

I hereby claim the benefit under 35 U.S.C. § 119(e) of any United States provisional application(s) listed below.

(Application Number)

(Filing Date)

207220 OF 9560

I hereby claim the benefit under 35 U.S.C. § 120 of any United States application(s), or § 365(c) of any PCT international application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT international application in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR § 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

(Application Number)	(Filing Date)	(Status--patented, pending, abandoned)
----------------------	---------------	--

(Application Number)	(Filing Date)	(Status--patented, pending, abandoned)
----------------------	---------------	--

I/we hereby appoint Practitioners at Customer Number 007470 as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith.

Address all correspondence to Customer No. 007470

Telephone No.: 212-819-8200; Facsimile No.: 212-354-8113

Please direct all telephone calls to John M. Genova, Esq., Direct Line - 212-819-8832.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believe to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of sole or first inventor (first name, middle initial, last name): Roland Nehl

Sole or first inventor's signature

Date:

Residence: Weilmünster, Germany

Citizenship: German

Post Office Address: Wiesenstrasse 33,  
D-35789 Weilmünster, Germany